IN THE CLAIMS:

The text of all pending claims (including withdrawn claims) is set forth below. Cancelled and not entered claims are indicated with claim number and status only. The claims as listed below show added text with underlining and deleted text with ~~strikethrough~~. The status of each claim is indicated with one of (original), (currently amended), (cancelled), (withdrawn), (new), (previously presented), or (not entered).

Please AMEND claims in accordance with the following:

1. (CURRENTLY AMENDED) A cipher designing apparatus for designing cipher logic of a cipher device that effects cipher or decryption per block by using an F-function for converting input bits to output bits using a plurality of S-boxes, said cipher designing apparatus comprising:

a selecting unit ~~which selects~~ selecting an input and output bit number of said plurality of S-boxes based on a memory capacity of a high-speed referable memory provided to said cipher device, a minimum input and output number of the S-boxes and an entire input and output number of the block, said selecting including determining an optimal combination of input and output bit numbers of each of the S-boxes for usable memory capacity of said memory; and

a S-box generating unit ~~which generates~~ generating a plurality of S-boxes each having the input and output bit number selected by said selecting unit.

2. (ORIGINAL) The cipher designing apparatus according to claim 1, further comprising a F-function generating unit which generates an F-function having said plurality of S-boxes generated by said S-box generating unit.

3. (ORIGINAL) The cipher designing apparatus according to claim 1, wherein said selecting unit selects the input and output bit number of each S-box in such a manner that a sum of sizes of said plurality of S-boxes becomes largest within a memory capacity of a primary cache memory installed in a processor provided to said cipher device.

4. (ORIGINAL) The cipher designing apparatus according to claim 3, wherein said selecting unit includes:

an input unit which inputs the memory capacity of said primary cache memory and an entire input and output bit number of said block;

a tentative decision unit which tentatively decides an input and output number of each S-box by generating an input and output number of each S-box by dividing the entire input and output bit number of said block inputted from said input unit and allocating a remainder to the input and output number of an arbitrary S-box; and

a combining unit which combines the input and output numbers of the S-boxes tentatively decided by said tentative decision unit within the memory capacity of said primary cache memory.

5. (ORIGINAL) The cipher designing apparatus according to claim 1, further comprising a smallest input and output number specifying unit which specifies a smallest value of the input and output number of said plurality of S-boxes.

6. (ORIGINAL) The cipher designing apparatus according to claim 4, wherein said combining unit completes combining of the input and output numbers based on a final value determined by the entire input and output bit number of said block and the memory capacity of said primary cache memory.

7. (ORIGINAL) The cipher designing apparatus according to claim 4, wherein said tentative decision unit tentatively decides the input and output number of each S-box by allocating said remainder, if there is any, to the input and output numbers of the S-boxes that are placed apart at remotest positions.

8. (CURRENTLY AMENDED) A cipher designing method for designing cipher logic of a cipher device that effects cipher or decryption per block by using an F-function for converting input bits to output bits using a plurality of S-boxes, the method comprising:

selecting an input and output bit number of said plurality of S-boxes based on a memory capacity of a high-speed referable memory provided to said cipher device, a minimum input and output number of the S-boxes and an entire input and output number of the block, said selecting including determining an optimal combination of input and output bit numbers of each of the S-boxes for usable memory capacity of said memory; and

generating a plurality of S-boxes each having the input and output bit number selected.

9. (PREVIOUSLY PRESENTED) The cipher designing method according to claim 8, further comprising:

generating an F-function having said plurality of S-boxes generated.

10. (PREVIOUSLY PRESENTED) The cipher designing method according to claim 8, wherein when the input and output bit number are selected, the input and output bit number of each S-box is selected in such a manner that a sum of sizes of said plurality of S-boxes becomes largest within a memory capacity of a primary cache memory installed in a processor provided to said cipher device.

11. (ORIGINAL) The cipher designing method according to claim 10, wherein selecting the input and output bit number includes:

inputting the memory capacity of said primary cache memory and an entire input and output bit number of said block;

tentatively deciding an input and output number of each S-box by generating an input and output number of each S-box by dividing the entire input and output bit number of said block inputted in the memory capacity and allocating a remainder to the input and output number of an arbitrary S-box; and

combining the input and output numbers of the S-boxes tentatively decided within the memory capacity of said primary cache memory.

12. (PREVIOUSLY PRESENTED) The cipher designing method according to claim 8, further comprising :

specifying a smallest value of the input and output number of said plurality of S-boxes.

13. (PREVIOUSLY PRESENTED) The cipher designing method according to claim 11, wherein the combining is completed based on a final value determined by the entire input and output bit number of said block and the memory capacity of said primary cache memory.

14. (PREVIOUSLY PRESENTED) The cipher designing method according to claim 11, wherein when tentatively deciding input and output number, the input and output number of each S-box is tentatively decided by allocating said remainder, if there is any, to the input and output numbers of the S-boxes that are placed apart at remotest positions.

15. (CURRENTLY AMENDED) A computer readable medium for storing instructions, which when executed by a computer, causes the computer to realizes a cipher designing method for designing cipher logic of a cipher device that effects cipher or decryption per block by using an F-function for converting input bits to output bits using a plurality of S-boxes, the method comprising:

selecting an input and output bit number of said plurality of S-boxes based on a memory capacity of a high-speed referable memory provided to said cipher device, a minimum input and output number of the S-boxes and an entire input and output number of the block, said selecting including determining an optimal combination of input and output bit numbers of each of the S-boxes for usable memory capacity of said memory; and

generating a plurality of S-boxes each having the input and output bit number selected.

16. (CURRENTLY AMENDED) A cipher designing method for designing cipher logic of a cipher device using an F-function to convert input bits to output bits via S-boxes, comprising:

generating a plurality of S-boxes each having an input and an output bit number selected based on memory capacity of a memory provided to the cipher device, the input and output bit number being selected by extracting a set of input and output numbers of the S-boxes as an optimal combination of input and output bit numbers based on an entire input and output bit number of a block and a minimum input and output number of the S-boxes; and

determining a combination set based on the memory capacity provided to the cipher device.

17. (CURRENTLY AMENDED) A method of designing cipher logic of a cipher device using an F-function for converting input bits to output bits, comprising:

determining an optimal input and output number of each of the S-boxes by generating a combination table having various sets of input and output numbers of the S-boxes enclosable in a memory of the cipher device and selecting an optimal combination of input and output numbers of each of the S-boxes; and

implementing the F-function by selecting ~~one of the sets~~ said optimal combination of input and output numbers of the S-boxes ~~in~~ from the combination table.